INTERN CAREER

WE SPEAK DATA

Cyber Security Internship Report

TASK 2: Incident Response Simulation

Content table

Introduction

The Incident Response Simulation task is designed to simulate a cybersecurity incident scenario to enhance incident response skills among interns. This exercise aims to provide practical experience in handling various cybersecurity incidents, such as malware attacks or phishing attempts, within a controlled environment. The simulation involves several key steps, including scenario creation, incident detection, response plan execution, forensic analysis, and post-incident assessment.

Please take the following in consideration :

- All company and IT team names used throughout this document are fictitious creations for demonstration purposes only. While some real company names are referenced, they are included solely to provide context and solidify the concepts presented.
- This report outlines a simulated phishing incident, highlighting potential attack methods and outcomes. It does not represent a real-world event.
- The two methods detailed within this report are based on real-world phishing tactics employed by attackers.

Overview about the task

This task simulates a cybersecurity incident to train and develop the skills of an incident response team. It involves creating a realistic scenario, assigning roles, practicing various response stages, and evaluating the overall effectiveness.

i. Scenario Creation

We will start by crafting a realistic cybersecurity incident. This could involve a malware attack infiltrating your systems or a phishing attempt targeting employees. We will define the context (where and how it happens), the attacker's objectives (data theft, disrupting operations), and the overall impact (one server or widespread infection).

ii. Incident Detection

Now, we will pretend we're monitoring your systems and identify the attack. This could involve assigning roles within your team (analysts, responders, decision-makers) and using pre-prepared logs or security software to simulate detecting suspicious activity, like unusual network traffic or unauthorized login attempts.

iii. Response Plan Execution

Once we've detected the incident, it's time to react. Here, our pre-defined plan comes into play. Team members following their assigned roles will take actions like isolating infected systems, containing the spread of the attack (like malware), and potentially shutting down critical systems to prevent further damage.

iv. Forensic Analysis

After containing the immediate threat, it's crucial to investigate what happened. This involves a deeper dive into affected systems and data. Imagine a team of forensic investigators examining digital footprints to pinpoint the attacker's entry point, the tools they used, and the extent of the breach. They'll also gather evidence like log files and compromised data samples for further analysis.

v. Post-Incident Assessment

The final step is crucial for improvement. The team gathers to review their response, analyze how effective the plan was, and identify areas where things could be improved. This is where valuable lessons are learned and incorporated to strengthen future incident response procedures.

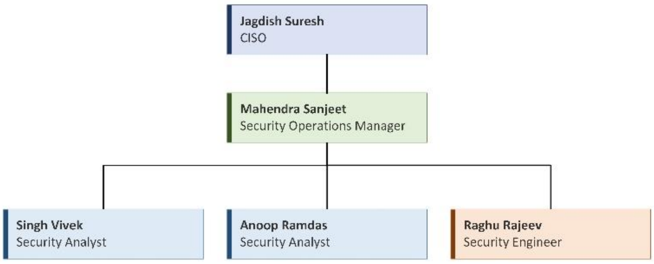


Figure 1: The IT Team in the simulation

I. 1st method: Creating an isolated environment for the test.

i. Scenario Creation

- SecureTech Solutions is a mid-sized company specializing in cybersecurity solutions. Our focus is on protecting businesses from cyber threats and securing sensitive data. While our finance department employees are not part of the IT team, they play a vital role in maintaining our company's security. We prioritize equipping them with the skills needed to identify and respond to cybersecurity incidents effectively. Through tailored training and simulations, we ensure that all employees contribute to our strong security posture.

SECURETECH™
UHD CAMERA

- In this scenario, we aim to assess the interns' ability in the finance department to detect and respond to a phishing email containing ransomware. We'll create a controlled environment using virtual machines (VMs) in VMware Workstation Pro, ensuring that the interns have access to the necessary tools and applications such as Microsoft 365 and Microsoft Edge. The VMs will be configured with Outlook to receive emails. The interns will receive two emails—one legitimate and one malicious—both related to an invoice review from a client. The malicious email will contain a disguised ransomware attachment, simulating a real-world cyber threat.

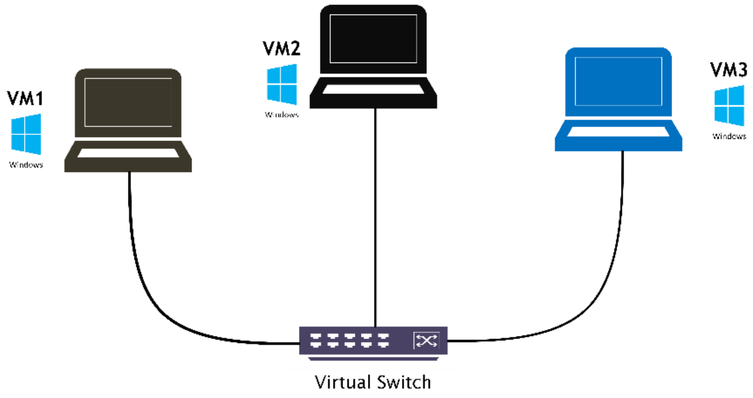


Figure 2: The test Environment in VMWare Workstation Pro.

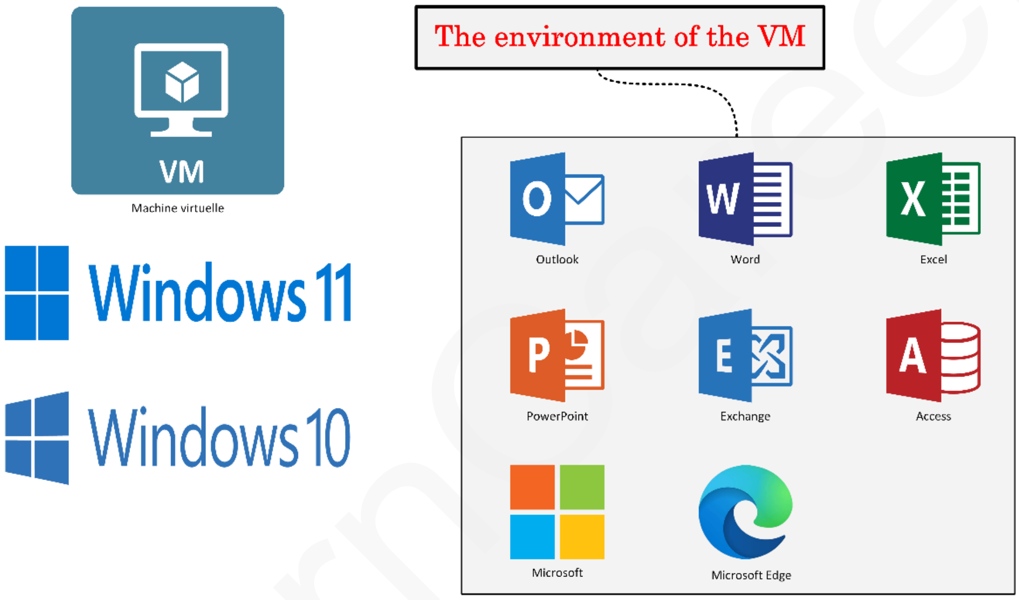
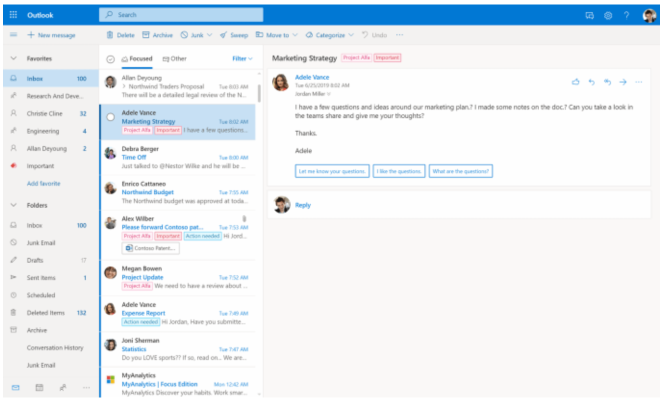


Figure 3: The services configured in each VM.

- ❖ We create an isolated virtual network in VMware Workstation Pro for the three VMs, ensuring they're disconnected from the company's real network while allowing communication between them. We configure Outlook on each VM to send and receive emails, setting up individual email accounts for the interns within the virtual environment. We craft two emails—one legitimate and one malicious—pertaining to invoice reviews, with the malicious email containing a disguised ransomware attachment. We send both emails to the interns' Outlook accounts on their respective VMs, ensuring successful delivery. We brief interns on the simulation scenario, emphasizing scrutiny of email authenticity and immediate reporting of suspicious emails.



Allan Deyoung
> Northwind Traders Proposal Tue 8:03 AM
There will be a detailed legal review of the N...

Adele Vance
Marketing Strategy Tue 8:02 AM
Project Alfa Important I have a few questions...

Debra Berger
Time Off Tue 8:00 AM
Just talked to @Nestor Wilke and he will be ...

Enrico Cattaneo
Northwind Budget Tue 7:55 AM
The Northwind budget was approved at toda...

Alex Wilber
Please forward Contoso pat... Tue 7:53 AM
Project Alfa Important Action needed Hi Jord...
Contoso Patent...

Megan Bowen
Project Update Tue 7:52 AM
Project Alfa We need to have a review about ...

Adele Vance
Expense Report Tue 7:49 AM
Action needed Hi Jordan, Have you submitte...

Joni Sherman
Statistics Tue 7:47 AM
Do you LOVE sports?? If so, read on... We are...

MyAnalytics
MyAnalytics | Focus Edition Mon 12:42 AM
MyAnalytics Discover your habits. Work smar...

Marketing Strategy Project Alfa Important

Adele Vance
Tue 6/25/2019 8:02 AM
Jordan Miller

I have a few questions and ideas around our marketing plan.? I made some notes on the doc.? Can you take a look in the teams share and give me your thoughts?

Thanks.

Adele

Let me know your questions. I like the questions. What are the questions?

Reply

Figure 4: Outlook Window Example

- ❖ During the simulation, three interns from the finance department received emails simultaneously on their respective VMs—one legitimate and one malicious. While one intern received a genuine email, the other two inadvertently opened the attachment in the malicious email, believing it to be legitimate. Consequently, ransomware executed on their laptops, encrypting files, and displaying ransom demands, compromising their systems.

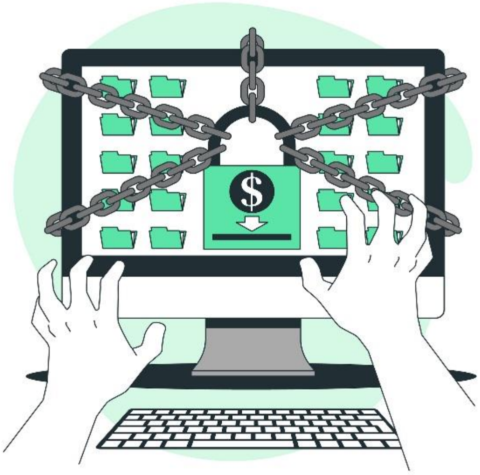
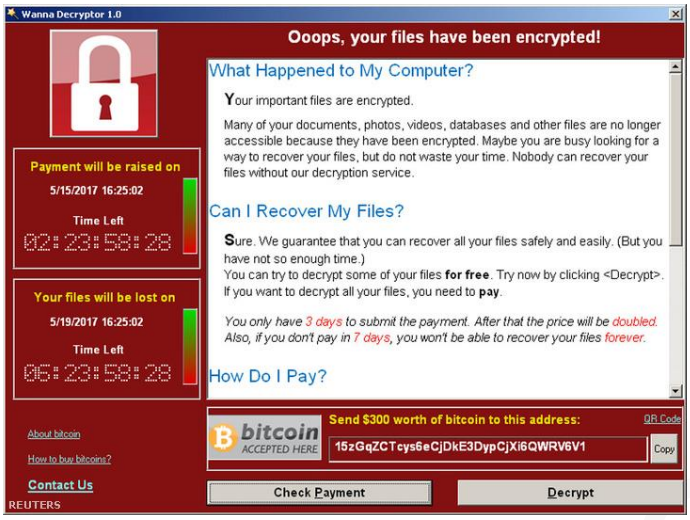


Figure 5: Ransomware attack illustration



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. (But you have not so enough time.)
You can try to decrypt some of your files **for free**. Try now by clicking <Decrypt>.
If you want to decrypt all your files, you need to **pay**.

You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.

How Do I Pay?

Payment will be raised on
5/15/2017 16:25:02
Time Left
02:23:58:28

Your files will be lost on
5/19/2017 16:25:02
Time Left
06:23:58:28

Send $300 worth of bitcoin to this address:
15zGqZCTcys6eCjDkE3DypCjXi6QWRV6V1

Figure 6: Ransomware Display on the interns VMs

ii. Incident Detection

- During the incident detection phase, the IT team utilized Security Information and Event Management (SIEM) tools to closely monitor the interns' actions and reactions to the simulated attack. Leveraging the SIEM's capabilities, they analyzed email logs, network traffic, and endpoint activities in real-time. The SIEM flagged suspicious behaviors, such as unusual email attachment accesses and file encryption patterns indicative of ransomware activity. By correlating these events with established threat indicators, the IT team swiftly identified that two of the interns had fallen victim to the phishing email and subsequent ransomware attack.

Here's the malicious mail that was used :

From: Finance Department of S.K. Logistics ***(J.keylon@sklogistiq.co)***

Non valid address

To: Finance Department of SecureTech Solutions

Subject: Urgent: Request for Complete Invoice

Spelling errors

Dear Finance Team,

We're writing to bring to your attention the incomplete invoice we received for the recent transaction. We require a full invoice with all necessary details, particularly the transaction number, which seems to be missing.

It is ***cruciale*** for our records and ***reconciliations*** processes to have accurate invoices, and the missing information is causing delays on our end.

Could you please ***prioritizes*** providing us with the complete invoice at your earliest convenience?

I have attached the incomplete invoice for your reference.

Thank you for your prompt attention to this matter.

Best regards,

S.K.
Logistics

Keylon June
Accountant in SK Logistics

The incomplete invoice.docx [The file containing the ransomware]

- Splunk ES is a comprehensive Security Information and Event Management (SIEM) platform. It acts as a central hub, ingesting and analyzing data from various security sources, including firewalls, email servers, and user activity logs. By leveraging advanced analytics and threat intelligence, Splunk ES empowers security teams to:
  - Gain Comprehensive Visibility: Splunk ES provides a unified view of security events across your organization, enabling a more holistic understanding of potential threats.
  - Detect Phishing Attempts in Real-Time: Advanced threat analytics within Splunk ES can identify suspicious email patterns, unusual attachments, and anomalies in user behavior that might indicate a phishing attempt.

- Investigate Incidents Efficiently: When a potential phishing attempt is detected, Splunk ES facilitates rapid investigation by providing a centralized platform to access and analyze all relevant data.
- Automate Threat Response: Splunk ES allows for automation of specific security tasks, such as quarantining suspicious emails or blocking malicious URLs, leading to quicker and more effective incident response.

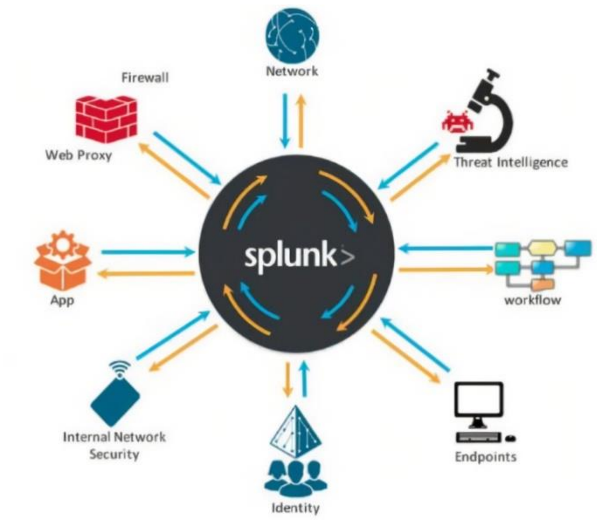


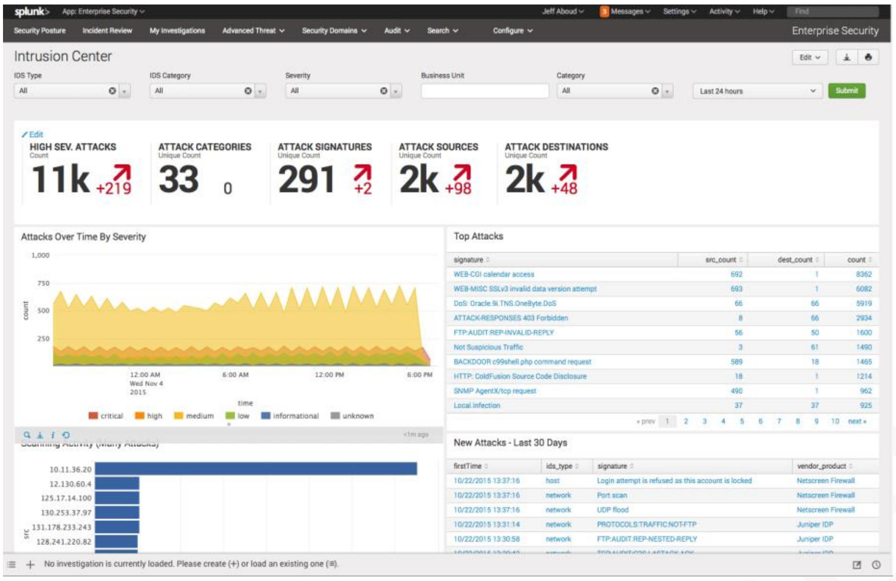
Figure 7: Splunk Enterprise Security

iii. Response Plan Execution

❖ In this simulated phishing attack scenario, the IT team will guide interns through the process of detecting, responding to, and mitigating a potential threat. By utilizing Splunk Enterprise Security (ES) and providing clear instructions, interns will learn to recognize phishing red flags, take immediate action, and report incidents promptly. Through hands-on experience and guidance from the IT team, interns will develop essential skills in cybersecurity incident response. Let's proceed with the step-by-step guide to navigate through this simulation effectively.

Step-by-step guide

1. Inform interns :
   - Gather interns for a briefing and clearly explain that this was a simulated phishing attack conducted in a controlled environment.
   - Introduce Splunk ES briefly, explaining that it helps detect phishing attempts without diving into technical details.
   - Review common phishing red flags to equip interns with identification skills.
2. Show Emails:
   - Display both the legitimate and malicious emails used in the simulation.
   - Legitimate Email: Show the interns the email with a clear sender, proper format, and expected content.
   - Phishing Email: Present the interns with the phishing email containing typos, urgency, suspicious sender address, and a seemingly legitimate attachment like a .pdf or .docx for example.
3. Inform Interns of Detection:
   - Inform interns that Splunk ES has detected a potential phishing attempt.
   - Simulate an alert by briefly showcasing how Splunk ES might present an alert for the suspicious email.



Intrusion Center

HIGH SEV. ATTACKS Count 11k +219

ATTACK CATEGORIES Unique Count 33 0

ATTACK SIGNATURES Unique Count 291 +2

ATTACK SOURCES Unique Count 2k +98

ATTACK DESTINATIONS Unique Count 2k +48

Attacks Over Time By Severity

Top Attacks

signature	src_count	dest_count	count
WEB-CGI calendar access	692	1	8362
WEB-MISC SSLv3 invalid data version attempt	693	1	6082
DoS: Oracle.9i.TNS.OneByte.DoS	66	66	5919
ATTACK-RESPONSES 403 Forbidden	8	66	2934
FTP:AUDIT:REP-INVALID-REPLY	56	50	1600
Not Suspicious Traffic	3	61	1490
BACKDOOR c99shell.php command request	589	18	1465
HTTP: ColdFusion Source Code Disclosure	18	1	1214
SNMP AgentX/tcp request	490	1	962
Local.Infection	37	37	925

New Attacks - Last 30 Days

firstTime	ids_type	signature	vendor_product
10/22/2015 13:37:16	host	Login attempt is refused as this account is locked	Netscreen Firewall
10/22/2015 13:37:16	network	Port scan	Netscreen Firewall
10/22/2015 13:37:16	network	UDP flood	Netscreen Firewall
10/22/2015 13:31:14	network	PROTOCOLS:TRAFFIC:NOT-FTP	Juniper IDP
10/22/2015 13:30:58	network	FTP:AUDIT:REP-NESTED-REPLY	Juniper IDP

No investigation is currently loaded. Please create (+) or load an existing one (≡).

Figure 8 : Splunk Enterprise Security Dashboard

- When Splunk Enterprise Security (Splunk ES) detects a potential phishing attempt, it initiates a series of automated actions to facilitate a swift and effective response. Here's a breakdown of the process:

1. Email Log Analysis with Search Processing Language (SPL):
   - Splunk ES ingests email server logs and leverages Search Processing Language (SPL) queries to analyze data related to emails, including:
     - Sender addresses: Identifying emails from unexpected or spoofed addresses often associated with phishing attempts.
     - Recipients: Unusual recipient lists or high outbound email volume from a single user might indicate compromised accounts.
     - Message content: Searching for keywords or phrases commonly used in phishing attempts, like urgency ("URGENT: Respond Now!"), threats ("Failure to comply will result in..."), or grammatical errors.

2. Email Content Analysis with Email Security Features:
   - Splunk ES utilizes pre-built email security features to analyze email content :
     - Subject line analysis: Searching for phishing keywords or suspicious phrases within the subject line.
     - Body text analysis: Identifying phishing URLs embedded within the email body or suspicious attachments like executables or compressed files.
     - Attachment analysis: Analyzing attachment metadata and file types to detect potentially malicious content. Splunk ES might also integrate with sandboxing tools to further analyze suspicious attachments in a safe environment.

3. Behavioral Analytics with User Entity Behavior Analytics (UEBA):
   - Splunk ES leverages User Entity Behavior Analytics (UEBA) to detect anomalies in user behavior related to email:
     - Email forwarding activity: Sudden spikes in outgoing emails, particularly to external addresses not typically used by the user, could indicate a compromised account forwarding sensitive information.
     - Email access patterns: Access to email accounts from unfamiliar locations or devices might suggest unauthorized access attempts associated with phishing campaigns.

4. Threat Intelligence Integration with Threat Intelligence Feeds :
   - Splunk ES can integrate with external threat intelligence feeds to enrich email analysis :
     - Domain reputation: Checking sender email addresses and embedded URLs against threat intelligence feeds to identify known malicious domains associated with phishing campaigns.

- Sender reputation analysis : Comparing sender IP addresses or email domains with blacklists or threat intelligence feeds to identify suspicious senders.

5. Alerting and Notification with Real-time Alerts :
   - Upon detecting suspicious email activity based on the combined analysis of these features, Splunk ES triggers real-time alerts.
   - These alerts can be configured to notify the IT security team via various channels, such as email, dashboard notifications, or Security Information and Event Management (SIEM) integrations.

4. Walkthrough Investigation:
   - Demonstrate how the IT team would investigate using Splunk ES :
     - Analyze email headers and content for red flags.
     - Compare email details with threat intelligence feeds.

5. Explain Importance of Immediate Action:
   - Stress the importance of quick response to prevent further damage.

6. Provide Instructions to interns:
   - Instruct interns to disconnect their infected laptops from the network to isolate the potential threat and prevent lateral movement within the network.
   - Advise interns not to interact further with the email or suspicious activity to avoid clicking links, downloading attachments, or opening suspicious files.
   - Encourage interns to report the incident immediately to the IT team for swift containment and remediation.

7. Specify Reporting Instructions:
   - Provide clear instructions on how to report, specifying who to contact (name, email address, phone number), and what information to provide (details of the email, suspicious activity observed).

iv. Forensic Analysis

- While Splunk Enterprise Security (Splunk ES) excels at detecting potential phishing attempts in real-time, it's not designed for in-depth forensic analysis. In the aftermath of a detected incident, security teams often need to delve deeper to understand the scope of the attack and gather evidence for potential legal or disciplinary actions. This is where digital forensics tools like Autopsy come into play.

Figure 9: Autopsy

- Autopsy is an open-source digital forensics platform developed by The Sleuth Kit Project. It provides a comprehensive suite of features to analyze digital evidence extracted from computers, mobile devices, and storage media. Security professionals leverage Autopsy for various forensic tasks, including:
  - Disk Image Analysis: Examining forensic copies of hard drives or storage devices to identify files, emails, and other relevant data.

- File System Analysis: Recovering deleted files, analyzing file access timestamps, and examining file metadata to reconstruct user activity.
- Email Analysis: Extracting and analyzing email content, attachments, and email headers to understand email communication patterns.
- Web History Analysis: Recovering browsing history and internet artifacts to identify websites accessed by the user.

❖ Here's a simplified guide for forensic analysis using Autopsy after SIEM detection:

Step-by-step guide : Preparation Phase

1. Secure Evidence: Isolate the affected laptops to prevent further data modification. Ideally, create a forensic disk image using tools like FTK Imager or similar software.
2. Gather Information: From SIEM data and user reports, note details like the suspicious email sender, attachment type (if any), and any user actions taken after interacting with the email.

Step-by-step guide : Autopsy Analysis Phase

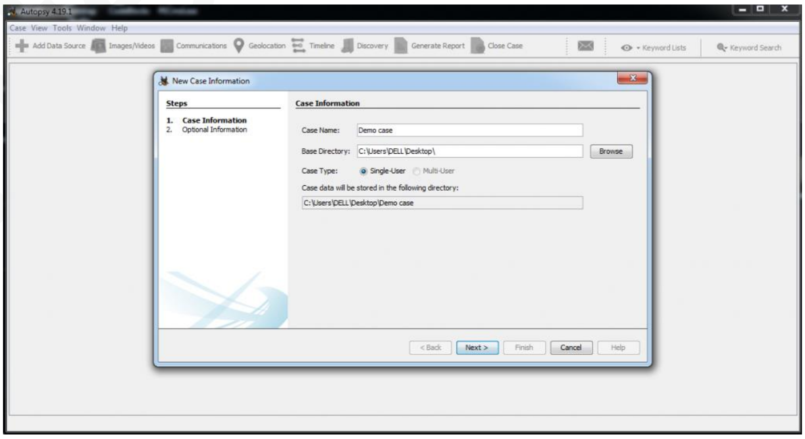
1. Open Autopsy : Launch Autopsy and choose *"New Case"* to create a new case for this incident.
2. Add the Disk Image : In the *"Add New Disk Image"* section, browse and select the forensic image of the isolated laptops hard drive.
3. Configure Analysis : Autopsy offers various ingest modules. Based on the information from SIEM, you can choose relevant options like:
   - Email Analysis: This can help identify email content related to the phishing attempt, including attachments.
   - File System Analysis: This allows examining downloaded files and access patterns.
   - Web History Analysis: If the user clicked a link, Autopsy can potentially recover browsing history.

4. Run Analysis : Click the *"Ingest"* button to initiate the analysis process. This may take some time depending on the size of the disk image.
5. Review Findings : Once complete, Autopsy displays the analysis results categorized by data types (emails, files, web history, etc.). Utilize filters and search functionalities to focus on areas relevant to the phishing attempt.

Focus Areas:

- *Emails:* Look for emails matching the sender and subject line identified through SIEM. Examine attachment details and recipient information.
- *Files:* Search for downloaded files, particularly around the time the user interacted with the email. Analyze file types and access timestamps.
- *Web History:* If a link was clicked, recovered browsing history might reveal the accessed website.

6. Generate Report : Based on your findings, generate a report documenting the analysis process, evidence identified (emails, files, etc.), and any potential conclusions about the phishing attempt's impact.



Case Name: Demo case

Base Directory: C:\Users\DELL\Desktop\

Case Type: ● Single-User ○ Multi-User

Case data will be stored in the following directory:

C:\Users\DELL\Desktop\Demo case

Figure 10: Autopsy Interface

v. Post-Incident Assessment

- Following the initial detection of a phishing attempt with Splunk ES and the potential forensic analysis using Autopsy, the IT team should conduct a thorough post-incident assessment. This assessment serves several critical purposes:
  - Evaluate Detection and Response Effectiveness: Review how Splunk ES performed in detecting the phishing attempt. Was it timely and accurate? Analyze the response timeline - were containment measures implemented swiftly to minimize damage?
  - Identify Root Causes and Vulnerabilities: Understand the underlying factors that allowed the phishing attempt to succeed. Was it a technical vulnerability (e.g., lack of email filtering) or a human factor (e.g., lack of user awareness)?
  - Improve Future Response: Based on the findings, identify areas for improvement in detection, containment, and user education to prevent similar incidents in the future.

Step-by-step guide : Post-Incident Assessment

1. Gather Information : Compile all relevant data, including:
   - Splunk ES alerts and investigation logs.
   - Autopsy analysis reports (if applicable).
   - User reports and interviews about their experience with the phishing email.
   - Any other relevant logs or security data.

2. Review and Analysis : The IT team thoroughly reviews the collected information to understand the following aspects:
   - Attack Vectors: How did the phishing attempt occur? What tactics were used (e.g., email spoofing, malicious attachments)?
   - Impact Assessment: Did the user click on the link or download the attachment? Was any data compromised?

- Success Factors: What factors allowed the attempt to (almost) succeed?
  - Were there weaknesses in email filtering?
  - Were users adequately trained to identify phishing attempts?

3. Develop Recommendations: Based on the analysis, the IT team identifies concrete recommendations for improvement:
   - Security Controls: Implementing additional email filtering rules or security awareness training.
   - User Education: Enhance user training to strengthen phishing identification skills and reporting procedures.
   - Technical Measures: Reviewing security configurations or deploying additional endpoint security solutions.

4. Reporting and Communication: The IT team documents the assessment findings and recommendations in a comprehensive report. This report is then communicated to relevant stakeholders, including management, and affected users.

II. 2nd method : Launching a phishing campaign.

i. What's KnowBe4 platform ?

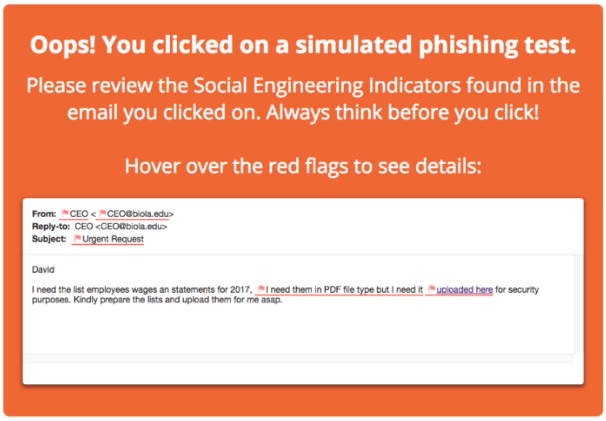
- KnowBe4 offers a user-friendly platform to launch safe and educational phishing simulations. These simulations mimic real-world phishing attempts, helping your employees identify red flags and avoid falling victim.
- KnowBe4's phishing simulation works like this: First, choose from pre-designed templates for different phishing scenarios. Then, customize the email content and sender address to make it look real but harmless. Next, target a specific group of users and run the simulation at a convenient time. Track user clicks and reports to see

how they react to the fake phishing attempt. Afterward, hold a training session using KnowBe4's resources to teach users about spotting phishing emails. The benefits include improved user awareness, lower risk of phishing attacks, measurable results on user susceptibility, and an easy-to-use platform for managing simulations.

Figure 11: KnowBe4

ii. Choose and Customize a Phishing Template

- Select a pre-built template aligned with your goals. KnowBe4 offers a library covering various scenarios.
- Modify the chosen template to create a realistic simulation:
  - Sender: Change the name to appear familiar (e.g., colleague with a typo) or impersonate a legitimate organization (avoid impersonating real people in authority).
  - Content: Edit the email body text while maintaining a harmless yet realistic tone. Include the phishing tactics you want to assess but avoid malware or malicious links.
  - Landing Page: Customize the landing page users reach upon clicking the phishing link. Design it to clearly indicate it's a simulation (e.g., display "This is a simulated phishing attempt").



Oops! You clicked on a simulated phishing test.

Please review the Social Engineering Indicators found in the email you clicked on. Always think before you click!

Hover over the red flags to see details:

From: CEO < CEO@biola.edu>
Reply-to: CEO <CEO@biola.edu>
Subject: Urgent Request

David

I need the list employees wages an statements for 2017, I need them in PDF file type but I need it uploaded here for security purposes. Kindly prepare the lists and upload them for me asap.

Figure 12: The pop-up when clicking on the phishing email

iii. Target Users and Timing

- Target Group: Select a representative group of users. Avoid targeting everyone at once. Consider user roles and susceptibility based on job duties or previous training.
- Timing: Schedule the simulation during typical work hours but avoid peak business times or holidays. This allows users more time to scrutinize the email.

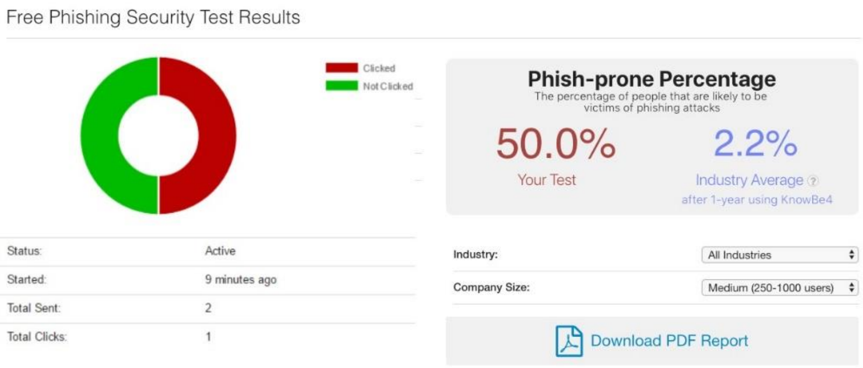
iv. Pre-Simulation Communication

- Inform users about the upcoming phishing simulation and its purpose (raising awareness, assessing susceptibility).
- Briefly explain the types of phishing attempts they might encounter and the reporting mechanism using KnowBe4's functionality.
- Emphasize there will be no repercussions for clicking or reporting.

v. Launching and Tracking

1. Launch the Phishing Simulation: Schedule the simulation using KnowBe4's platform.
2. Track User Reactions: KnowBe4 monitors user behavior:
   - Clicks: Identify users who clicked the phishing link in the email.

- Reports: Track users who reported the email as suspicious using KnowBe4's reporting feature.



Free Phishing Security Test Results

Status:	Active
Started:	9 minutes ago
Total Sent:	2
Total Clicks:	1

Phish-prone Percentage

The percentage of people that are likely to be victims of phishing attacks

50.0% Your Test

2.2% Industry Average after 1-year using KnowBe4

Industry: All Industries

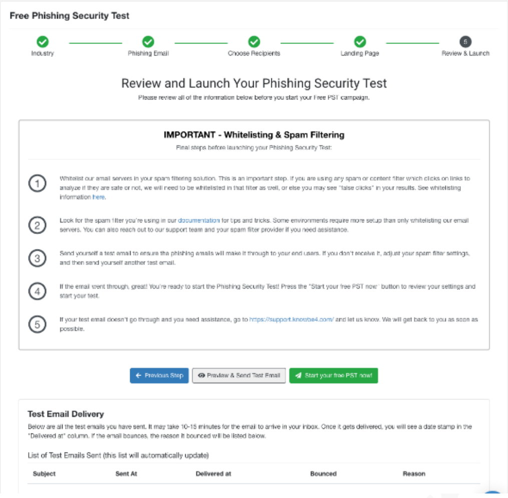
Company Size: Medium (250-1000 users)

Figure 13: The results of a test

vi. Post-Simulation Activities

- Data Analysis: Analyze the simulation results:
  - How many users clicked the phishing link?
  - How many users reported the suspicious email?
  - Did the simulation identify areas needing user training improvements?
- Debriefing Session: Conduct a training session for all users:
  - Discuss the simulation scenario and the phishing tactics employed.
  - Explain why the email was a phishing attempt (e.g., sender inconsistencies, urgency tactics, generic greetings).
  - Showcase the simulated landing page users would have seen if they clicked the link.
  - Emphasize the importance of reporting suspicious emails to the IT team.
  - Encourage questions and clarify doubts about phishing identification.
  - Phishing Quiz (Optional): Consider administering a short phishing quiz using KnowBe4 to assess user knowledge retention after the training session.

- Ongoing Security Awareness: Schedule regular training sessions to keep users updated on evolving phishing tactics and best practices for staying safe online.



Review and Launch Your Phishing Security Test

Please review all of the information below before you start your Free PST campaign.

IMPORTANT - Whitelisting & Spam Filtering

Final steps before launching your Phishing Security Test:

1. Whitelist our email servers in your spam filtering solution. This is an important step. If you are using any spam or content filter which clicks on links to analyze if they are safe or not, we will need to be whitelisted in that filter as well, or else you may see "false clicks" in your results. See whitelisting information here.
2. Look for the spam filter you're using in our documentation for tips and tricks. Some environments require more setup than only whitelisting our email servers. You can also reach out to our support team and your spam filter provider if you need assistance.
3. Send yourself a test email to ensure the phishing emails will make it through to your end users. If you don't receive it, adjust your spam filter settings, and then send yourself another test email.
4. If the email went through, great! You're ready to start the Phishing Security Test! Press the "Start your free PST now" button to review your settings and start your test.
5. If your test email doesn't go through and you need assistance, go to https://support.knowbe4.com/ and let us know. We will get back to you as soon as possible.

Test Email Delivery

Below are all the test emails you have sent. It may take 10-15 minutes for the email to arrive in your inbox. Once it gets delivered, you will see a date stamp in the "Delivered at" column. If the email bounces, the reason it bounced will be listed below.

List of Test Emails Sent (this list will automatically update)

Subject	Sent At	Delivered at	Bounced	Reason

Figure 14: Finalizing the setup of a campaign

Conclusion

- Phishing simulations are a crucial tool for raising user awareness and improving their ability to identify and avoid phishing attempts.

However, when deciding how to conduct these simulations, you have two methods:

- Launching a phishing campaign on KnowBe4: This user-friendly platform offers a variety of pre-built templates and simplifies the process of launching simulations.
- Creating an isolated environment for test: This approach utilizes virtual machines to create a more realistic network environment and integrates security tools for advanced analysis.

- Let's delve into the pros and cons of each method to help you determine which one is the most effective for your organization.

Method 1 : Creating an isolated environment for test

Pros :

- Highly realistic simulation environment replicating a network.
- Allows for targeted attacks based on user roles.
- Can demonstrate lateral movement and vulnerability exploitation (educational purposes only).
- Integrates security tools like Splunk ES for real-time insights.
- Provides opportunity to showcase Autopsy's forensic analysis capabilities.

Cons :

- Requires more technical expertise to set up and manage.
- More time-consuming to develop and configure compared to KnowBe4.
- May be cost-prohibitive for smaller organizations.
- Less user-friendly for those unfamiliar with virtual environments and security tools.

Method 2 : Launching a phishing campaign

Pros :

- User-friendly platform for launching phishing simulations.
- Wide range of pre-built templates covering various scenarios.
- Easy to track user clicks, reports, and completion rates.
- Less technical expertise required to set up and manage.
- Cost-effective solution for most organizations.

Cons :

- Limited customization options compared to a custom-built simulation.
- Lacks the realism of a completely isolated virtual environment.
- Doesn't involve security tools.

Comparative Table between the 2 methods

Factor	Method 1	Method 2
Ease of Use	Easy	Complex
Cost	Cost-effective	More expensive
Realism	Moderate	High
User Focus	User education	Advanced training
Technical Expertise	Low	High

❖ By carefully weighing these factors, you can choose the phishing simulation method that best suits your organization's needs and helps you develop a more secure and aware user base.

List of figures